



## CHAPTER 39

# Configuring the Switch Access Using AAA

This chapter describes how to configure authentication, authorization, and accounting (AAA) to monitor and control access to the command-line interface (CLI) on the Catalyst 6500 series switches.



### Note

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference*



For information on configuring 802.1X authentication to restrict unauthorized devices from connecting to a LAN through publicly accessible ports, see [Chapter 40, “Configuring 802.1X Authentication.”](#)



For information on configuring MAC address authentication bypass, see [Chapter 41, “Configuring MAC Authentication Bypass.”](#)



For information on configuring ports to allow or restrict traffic based on host MAC addresses, see [Chapter 38, “Configuring Port Security.”](#)



For information on configuring network admission control, see [Chapter 44, “Configuring Network Admission Control.”](#)

This chapter consists of these sections:

- [Understanding How Authentication Works, page 39-2](#)  
[Configuring Authentication on the Switch, page 39-9](#)  
[Understanding How Authorization Works, page 39-44](#)  
[Configuring Authorization on the Switch, page 39-46](#)  
[Understanding How Accounting Works, page 39-52](#)  
[Configuring Accounting on the Switch, page 39-55](#)

# Understanding How Authentication Works

- [Authentication Overview, page 39-2](#)
- [Understanding How Login Authentication Works, page 39-2](#)
- [Understanding How Local Authentication Works, page 39-3](#)
- [Understanding How Local User Authentication Works, page 39-3](#)
- [Understanding How TACACS+ Authentication Works, page 39-4](#)
- [Understanding How RADIUS Authentication Works, page 39-5](#)
- [Understanding How Kerberos Authentication Works, page 39-5](#)

## Authentication Overview

You can configure any combination of these authentication methods to control access to the switch:

- Login authentication
- Local authentication
- RADIUS authentication
- TACACS+ authentication
- Kerberos authentication



### Note

---

Kerberos authentication does not work if TACACS+ is used as the authentication method.

---

When you enable local authentication with one or more other authentication methods, local authentication is always attempted last. However, you can specify different authentication methods for the console and Telnet connections. For example, you might use local authentication for the console connections and RADIUS authentication for the Telnet connections.

## Understanding How Login Authentication Works

**set authentication login attempt *count*** command. Enter the **set authentication enable attempt** command to set the login limits for accessing enable mode. The configurable range is three (default) to ten tries. Setting the login authentication limit to zero (0) disables this function.

All authentication methods are supported (RADIUS, TACACS+, Kerberos, or local).

You can configure the lockout (delay) time from the CLI and SNMP through the **set authentication login lockout** **set authentication enable lockout**

The configurable range is 30–43200 seconds. Setting the lockout time to zero (0) disables this function.

---

If you are locked out at the console, the console does not allow you to log in during that lockout time. If you are locked out with a Telnet session, the connection closes when the time limit is reached. The switch closes any subsequent access from that station during the lockout time and provides an appropriate notice.

## Understanding How Local Authentication Works

Local authentication uses locally configured login and enable passwords to authenticate login attempts. The login and enable passwords are local to each switch and are not mapped to the individual usernames.

By default, local authentication is enabled. You can disable local authentication after enabling one or more of the other authentication methods. However, when local authentication is disabled, if you disable all other authentication methods, local authentication is reenabled automatically.

You can enable local authentication and one or more of the other authentication methods at the same time. The switch attempts local authentication only if the other authentication methods fail.

## Understanding How Local User Authentication Works

Local user authentication uses local user accounts and passwords that you create to validate the login attempts of local users. Each switch can have a maximum of 25 local user accounts. Before you can enable local user authentication, you must define at least one local user account.

You set up local user accounts by creating a unique username and password combination for each local user. Each username must be fewer than 65 characters and can be any alphanumeric character (at least one character must be alphabetic).

You configure each local user account with a privilege level; the valid privilege levels are 0 or 15. The privilege level assigned to a username and password combination designates whether a user will be logged in to normal or privileged mode after successful authentication. A user with a privilege level of 0 is automatically logged in to normal mode, and a user with a privilege level of 15 is logged in to privileged mode. A user with a privilege level of 0 can still access privileged mode by entering the command and password combination. Once a local user is logged in, only the commands that are available for that privilege level can be displayed.



---

If you are running a CiscoView image or are logging in using an HTTP login, the system completes its initial authentication using the username and password combination. You can enter privileged mode by either providing the privilege password or using the username and password combination if the local user has a privilege level of 15.

---

---

## Understanding How TACACS+ Authentication Works

- 

- 

- 

- 

- 

- 

- 

- 

- 

- 

-

## Understanding How RADIUS Authentication Works



Note

- 
- 
- 
- 
- 
- 
- 

primary

## Understanding How Kerberos Authentication Works

**Table 39-1 Kerberos Terminology**

Term	Definition
	Authentication tickets, such as ticket granting tickets (TGTs), and service credentials. Kerberos credentials verify the ticket of a user or service. If a network service decides to trust the Kerberos server that issued the ticket, the Kerberos credential can be used in place of retyping in a username and password. Credentials have a default life span of eight hours.
Kerberos identity	(See Kerberos principal.)
Kerberos principal	The Kerberos principal is who you are or what a service is according to the Kerberos server. (Also known as a Kerberos identity.)
Kerberos realm	A domain consisting of users, hosts, and network services that are registered to a Kerberos server. The Kerberos server is trusted to verify the identity of a user or network service to another user or network service. Kerberos realms must always be in uppercase characters.
Kerberos server	A daemon running on a network host. Users and network services register their identity with the Kerberos server. Network services query the Kerberos server to authenticate to other network services.
Key distribution center (KDC)	A Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.
Service credential	A credential for a network service. When issued from the KDC, this credential is encrypted with the password that is shared by the network service and the KDC and with the user's TGT.
SRVTAB	A password that a network service shares with the KDC. The network service authenticates an encrypted service credential by using the SRVTAB (also known as a KEYTAB) to decrypt it.
Ticket granting ticket (TGT)	A credential that the KDC issues to authenticated users. When users receive a TGT, they can authenticate to network services within the Kerberos realm that is represented by the KDC.

In the Catalyst 6500 series switches, the Telnet clients and servers through both the console and in-band management port can be Kerberized.



Kerberos authentication does not work if TACACS+ is used as the authentication mechanism.

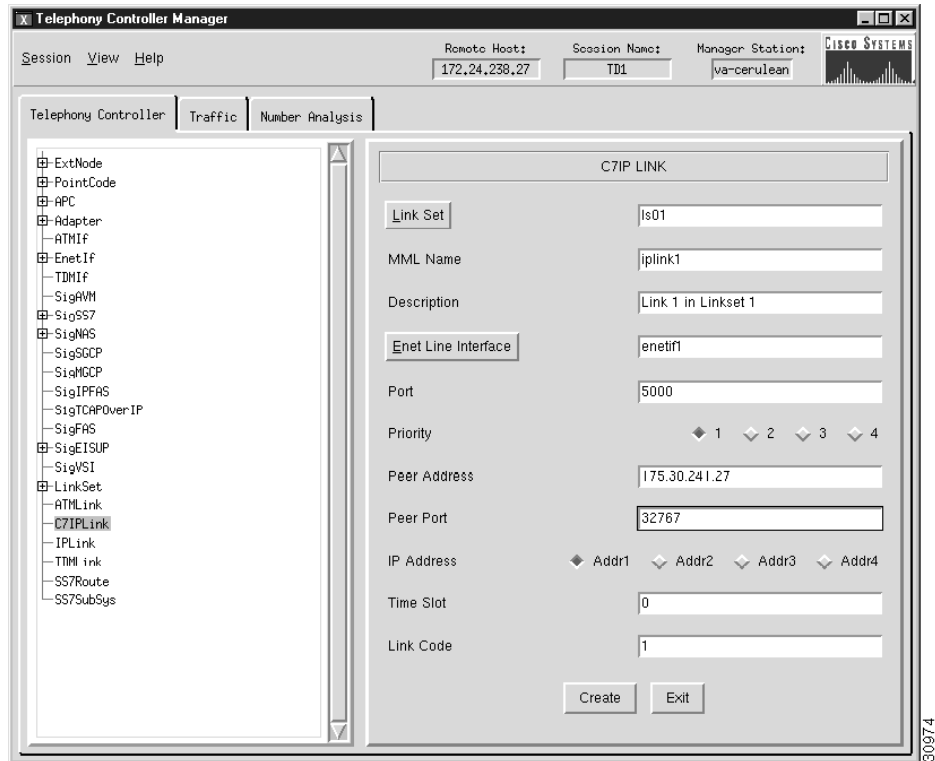


If you are logged in to the console through a modem or a terminal server, you cannot use a Kerberized login procedure.

## Using a Kerberized Login Procedure

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.

Figure 39-1 Kerberized Telnet Connection

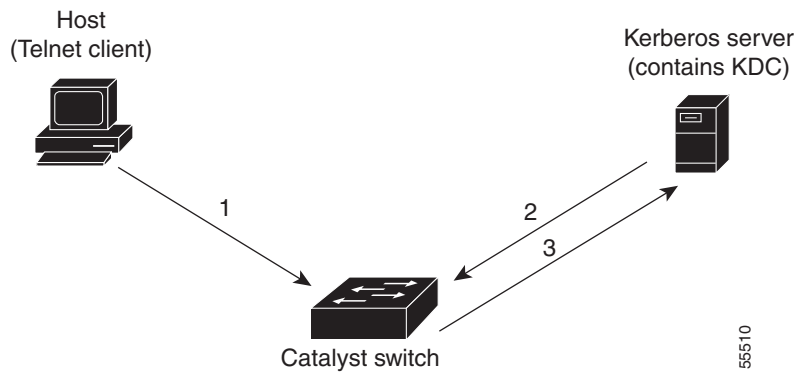


## Using a Non-Kerberized Login Procedure

  
Note

- 1.
- 2.
- 3.
- 4.
- 5.

**Figure 39-2**     *Non-Kerberized Telnet Connection*



## Configuring Authentication on the Switch

- 
- 
- 
- 
- 

, page 39-17



## Authentication Configuration Guidelines

- 
- 
- 
- 
- 
- 
- 
- 

## Configuring Login Authentication

- 
- 

## Setting Authentication Login Attempts on the Switch

Task	Command
Step 1	[ ] { }
Enable the login lockout time on the switch. Enter the or keyword if you want to enable local authentication only for the console port or for Telnet connection attempts.	[ ] { } [ ]
Verify the local authentication configuration.	<b>show authentication</b>

This example shows how to limit login attempts to 5, set the lockout time for both console and Telnet connections to 50 seconds, and verify the configuration:

```

Console> (enable) set authentication login attempt 5
Login authentication attempts for console and telnet logins set to 5.
Console> (enable) set authentication login lockout 50
Login lockout time for console and telnet logins set to 50.
Console> (enable) show authentication

```

```

Login Authentication: Console Session  Telnet Session  Http Session
-----
tacacs                disabled        disabled        disabled
radius                disabled        disabled        disabled
kerberos              disabled        disabled        disabled
local                 enabled(primary)  enabled(primary)  enabled(primary)
attempt limit         5              5              -
lockout timeout (sec) 50             50             -

```

```

Enable Authentication: Console Session  Telnet Session  Http Session
-----
tacacs                disabled        disabled        disabled
radius                disabled        disabled        disabled
kerberos              disabled        disabled        disabled
local                 enabled(primary)  enabled(primary)  enabled(primary)
attempt limit         3              3              -
lockout timeout (sec) disabled        disabled        -
Console> (enable)

```

## Setting Authentication Login Attempts for the Privileged Mode

	Task	Command
Step 1		
Step 2		
Step 3		

```

set authentication enable attempt 5

set authentication enable lockout 50

```

```
show authentication
```

## Configuring Local Authentication

- 
- 
- 
- 
- 

## Enabling Local Authentication



Note

Task	Command
Step 1	http   telnet
console telnet	set authentication enable local enable all console http   telnet
	show authentication



<b>Return</b>	<b>set password</b>

```
          set password
Enter old password: <old_password>
                  <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)
```



Task	Command

```
Enter old password: <  
Enter new password: <  
Retype new password: <  
Password changed.  
Console> (enable)
```

## Disabling Local Authentication



Caution

	Task	Command
Step 1		
Step 2		
Step 3		



**Note**

---

---

## Recovering a Lost Password

---

**Step 1**

**Step 2**

**Step 3**

**Step 4**

**Step 5**

**Step 6**

**Step 7**

**Step 8**

---

# Configuring Local User Authentication

- 
- 
- 
- 

## Creating a Local User Account

	<i>pwd</i>
	<b>privilege</b> <i>privilege_level</i>

```
set localuser user picard password captain privilege 15
```

```
show localusers
```

```
Local User Authentication: disabled
Username                   Privilege Level
-----
picard                      15
Console> (enable)
```


```
Console> (enable)
Local User Authentication enabled.
Console> (enable)
Login Authentication:  Console Session  Telnet Session  Http Session
-----
tacacs                 disabled        disabled        disabled
radius                 disabled        disabled        disabled
```

```

local *                enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                    3                    -
lockout timeout (sec) disabled                disabled                -

Enable Authentication: Console Session  Telnet Session  Http Session
-----
tacacs                 disabled        disabled        disabled
radius                 disabled        disabled        disabled
kerberos               disabled        disabled        disabled
local *                enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                    3                    -
lockout timeout (sec) disabled                disabled                -
* Local User Authentication enabled.
Console> (enable)

```


```

Console> (enable)
local user authentication set to disable.
Console> (enable)
Login Authentication: Console Session  Telnet Session  Http Session
-----
tacacs                 disabled        disabled        disabled
radius                 disabled        disabled        disabled
kerberos               disabled        disabled        disabled
local *                enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                    3                    -
lockout timeout (sec) disabled                disabled                -

Enable Authentication: Console Session  Telnet Session  Http Session
-----
tacacs                 disabled        disabled        disabled
radius                 disabled        disabled        disabled
kerberos               disabled        disabled        disabled
local *                enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                    3                    -
lockout timeout (sec) disabled                disabled                -
* Local User Authentication disabled.
Console> (enable)

```

	Task	Command
Step 1		
Step 2		

```

Console> (enable)
Local user cleared.
Console> (enable)
Local User Authentication: enabled
Username                               Privilege Level
-----                               -
picard                                  15
number1                                 0
worf                                     15
troy                                     0
Console> (enable)

```

## Specifying TACACS+ Servers


```

      set tacacs server 172.20.52.3
172.20.52.3 added to TACACS server table as primary server.
Console> (enable) set tacacs server 172.20.52.2 primary

      set tacacs server 172.20.52.10

      show tacacs

```

```

Tacacs direct request: disabled
Tacacs-Server                               Status
-----
172.20.52.3
172.20.52.2                                primary
172.20.52.10
Console> (enable)

```




```

Console> (enable)
tacacs login authentication set to enable for console and telnet session.
Console> (enable)
tacacs enable authentication set to enable for console and telnet session.
Console> (enable)

```

```

Login Authentication: Console Session Telnet Session
-----
tacacs                enabled(primary) enabled(primary)
radius                disabled           disabled
local                 enabled           enabled

```

```

Enable Authentication: Console Session Telnet Session
-----
tacacs                enabled(primary) enabled(primary)
radius                disabled           disabled
local                 enabled           enabled
Console> (enable)

```




---



---

	<i>key</i>

```

set tacacs key Secret_TACACS_key
The tacacs key has been set to Secret_TACACS_key.
Console> (enable) show tacacs
Tacacs key: Secret_TACACS_key
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled

Tacacs-Server                               Status
-----
172.20.52.3
172.20.52.2                                primary
172.20.52.10
Console> (enable)

```

## Specifying the TACACS+ Timeout Interval

	Task	Command
Step 1		
Step 2		

## Specifying the TACACS+ Login Attempts

	Task	Command
Step 1		<i>number</i>

## Enabling TACACS+ Directed Request

When directed request is enabled, you can optionally

	<b>set tacacs directedrequest enable</b>
	<b>show tacacs</b>

```
set tacacs directedrequest enable  
show tacacs
```

	<b>set tacacs directedrequest disable</b>
	<b>show tacacs</b>

<b>all</b>	<b>clear tacacs server all</b>
	<b>show tacacs</b>

	<b>clear tacacs key</b>
	<b>show tacacs</b>

<b>console telnet</b>	<b>set authentication login tacacs disable all console http telnet</b>
<b>console telnet</b>	<b>set authentication enable tacacs disable all console http telnet</b>
	<b>show authentication</b>

	<b>auth-port</b>
	<b>primary</b>
	<b>show radius</b>

172.20.52.3 with auth-port 1812 added to radius server table as primary server.  
 Console> (enable)

```

Login Authentication: Console Session Telnet Session
-----
tacacs                disabled          disabled
radius                disabled          disabled
local                 enabled(primary) enabled(primary)
Enable Authentication: Console Session Telnet Session
-----
tacacs                disabled          disabled
radius                disabled          disabled
local                 enabled(primary) enabled(primary)

```

```

Radius Deadtime:      0 minutes
Radius Key:
Radius Retransmit:   2
Radius Timeout:      5 seconds

```

```

Radius-Server          Status Auth-port
-----
172.20.52.3           primary 1812

```

Console> (enable)




---



---


```

Console> (enable) set radius key Secret_RADIUS_key
Radius key set to Secret_RADIUS_key
Console> (enable) show radius
Login Authentication: Console Session   Telnet Session
-----
tacacs                disabled          disabled
radius                enabled(primary) enabled(primary)
local                 enabled           enabled

Enable Authentication: Console Session   Telnet Session
-----
tacacs                disabled          disabled
radius                enabled(primary) enabled(primary)
local                 enabled           enabled

Radius Deadtime:           0 minutes
Radius Key:                Secret_RADIUS_key
Radius Retransmit:        2
Radius Timeout:           5 seconds

Radius-Server              Status   Auth-port
-----
172.20.52.3                primary  1812
Console> (enable)

```



Enable RADIUS authentication for normal login mode. Enter the <code>enable</code> or <code>enable</code> keyword if you want to enable RADIUS only for the console port or Telnet connection attempts.	<code>enable</code> [ <code>enable</code> ]
Enable RADIUS authentication for enable mode. Enter the <code>enable</code> or <code>enable</code> keyword if you want to enable RADIUS only for the console port or Telnet connection attempts.	<code>enable</code> [ <code>enable</code> ]
Create a user \$enab15\$ on the RADIUS server and assign a password to that user.	See the Note below for additional information.
Verify the RADIUS configuration.	



To use RADIUS `enable` for enable mode, you must create a user \$enab15\$ on the RADIUS server and assign a password to that user. This user needs to be created in addition to your assigned username and password on the RADIUS server (for example, the username is john, and the password is hello). After you log in to the Catalyst 6500 series switch with your assigned username and password (john/hello), you can enter enable mode using the password that is assigned to the \$enab15\$ user.

If your RADIUS server does not support the \$enab15\$ username, you can set the service-type attribute (attribute 6) to Administrative (value 6) for a RADIUS user to directly launch the user into enable mode without asking for a separate enable password.

This example shows how to enable RADIUS authentication and verify the configuration:

You can specify the timeout interval between the retransmissions to the RADIUS server. The default timeout is 5 seconds.

To specify the RADIUS timeout interval, perform this task in privileged mode:

Specify the RADIUS timeout interval.	
Verify the RADIUS configuration.	

This example shows how to specify the RADIUS timeout interval and verify the configuration:

You can specify the number of times that the switch will attempt to contact a RADIUS server before the next configured server is tried. By default, each RADIUS server is tried two times.

To specify the RADIUS retransmit count, perform this task in privileged mode:

Specify the RADIUS server retransmit count.	
Verify the RADIUS configuration.	

This example shows how to specify the RADIUS retransmit count and verify the configuration:

**set radius retransmit 4**

Radius retransmit count set to 4.

Console> (enable)

Login Authentication:	Console Session	Telnet Session
-----	-----	-----
tacacs	disabled	disabled
radius	enabled(primary)	enabled(primary)
local	enabled	enabled
Enable Authentication:	Console Session	Telnet Session
-----	-----	-----
tacacs	disabled	disabled
radius	enabled(primary)	enabled(primary)
local	enabled	enabled

Radius Deadtime: 0 minutes  
Radius Key: Secret\_RADIUS\_key  
Radius Retransmit: 4  
Radius Timeout: 10 seconds

Radius-Server	Status	Auth-port
-----	-----	-----
172.20.52.3	primary	1812

Console> (enable)


Console> (enable)  
Radius deadtime set to 5 minute(s)  
Console> (enable)

Login Authentication:	Console Session	Telnet Session
-----	-----	-----
tacacs	disabled	disabled
radius	enabled(primary)	enabled(primary)
local	enabled	enabled

```

Enable Authentication: Console Session   Telnet Session
-----
tacacs                disabled          disabled
radius                enabled(primary)  enabled(primary)
local                enabled          enabled

Radius Deadtime:           5 minutes
Radius Key:                Secret_RADIUS_key
Radius Retransmit:        4
Radius Timeout:           10 seconds

Radius-Server             Status   Auth-port
-----
172.20.52.3              primary  1812
172.20.52.2              1812
Console> (enable)

```

## Specifying Optional Attributes for RADIUS Servers

You can specify optional attributes in the RADIUS ACCESS\_REQUEST packet. The `radius-server` command allows you to specify the transmission of certain optional attributes such as Framed-IP address, NAS-Port, Called-Station-Id, Calling-Station-Id, and so on. You can set attribute transmission by either the attribute number or the attribute name. Transmission of the attributes is disabled by default.




---

Software release 7.5(1) supports only the Framed-IP address (Attribute 8).

---

To specify the optional attributes for the RADIUS server, perform this task in privileged mode:


This example shows how to specify and enable the Framed-IP address attribute by number and verify the configuration:

```

set radius attribute 8 include-in-access-req enable
Transmission of Framed-ip address in access-request packet is enabled.
Console> (enable)
RADIUS Deadtime:           0 minutes
RADIUS Key:                123456
RADIUS Retransmit:        2
RADIUS Timeout:           5 seconds
Framed-IP Address Transmit: Enabled

RADIUS-Server             Status   Auth-port   Acct-port
-----
10.6.140.230             primary  1812        1813
Console> (enable)

```

```

Console> (enable) set radius attribute framed-ip-address include-in-access-req disable
Transmission of Framed-ip address in access-request packet is disabled.
Console> (enable)

```


```

Console> (enable) clear radius server 172.20.52.3
172.20.52.3 cleared from radius server table.
Console> (enable)

```

```

Console> (enable) clear radius server all
All radius servers cleared from radius server table.
Console> (enable)

```


```

Console> (enable) clear radius key
Radius key cleared.
Console> (enable) show radius

```

```

Login Authentication: Console Session  Telnet Session
-----
tacacs                disabled          disabled
radius                disabled          disabled
local                 enabled(primary) enabled(primary)

Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled          disabled
radius                disabled          disabled
local                 enabled(primary) enabled(primary)

```

```

Radius Deadtime:          0 minutes
Radius Key:
Radius Retransmit:       2
Radius Timeout:          5 seconds

Radius-Server             Status   Auth-port
-----
172.20.52.3               primary 1812
Console> (enable)

```


```

Console> (enable) set authentication login radius disable
radius login authentication set to disable for console and telnet session.
Console> (enable) set authentication enable radius disable
radius enable authentication set to disable for console and telnet session.
Console> (enable) show authentication

```

```

Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius                disabled      disabled
local                 enabled(primary)  enabled(primary)

Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius                disabled      disabled
local                 enabled(primary)  enabled(primary)
Console> (enable)

```



---

---

---

```
/usr/local/sbin/kdb5_util create -r CISCO.EDU -s
```

```
ank host/Cat6509.cisco.edu@CISCO.EDU
```

```
ank user1@CISCO.EDU
```

```
ank user1/admin@CISCO.EDU
```

**admin.local ktadd**

```
ktadd host/Cat6509.cisco.edu@CISCO.EDU
```

```
/usr/local/sbin/krb5kdc  
/usr/local/sbin/kadmind
```

---

	<b>set authentication login kerberos enable all console http telnet primary</b>
	<b>show authentication</b>

```
kerberos> (enable)
kerberos login authentication set to enable for telnet session.
kerberos> (enable)
```

```
Login Authentication: Console Session  Telnet Session
-----
tacacs                disabled          disabled
radius               disabled          disabled
kerberos             disabled          enabled(primary)
local                enabled(primary) enabled
```

```
Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled          disabled
radius               disabled          disabled
kerberos             disabled          enabled(primary)
local                enabled(primary) enabled
kerberos> (enable)
```

```
kerberos> (enable)
kerberos login authentication set to enable for console session.
kerberos> (enable)
```

```
Login Authentication: Console Session  Telnet Session
-----
tacacs                disabled          disabled
radius               disabled          disabled
kerberos             enabled(primary) enabled(primary)
local                enabled          enabled
```

```
Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled          disabled
radius               disabled          disabled
kerberos             enabled(primary) enabled(primary)
local                enabled          enabled
kerberos> (enable)
```




```

kerberos> (enable) set kerberos local-realm CISCO.COM
Kerberos local realm for this switch set to CISCO.COM.
kerberos> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM, Server:187.0.2.1, Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com, Realm:CISCO.COM

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/niners.cisco.com@CISCO.COM 0 932423923 1 1 8 01;;8>00>50;0=0=0
kerberos> (enable)

```

	<i>hostname  </i>
	<i>ip_address port</i>
	<i>kerberos_realm hostname</i>
	<i>  ip_address port</i>

```
kerberos> (enable)
Kerberos Realm-Server-Port entry set to:CISCO.COM - 187.0.2.1 - 750
kerberos> (enable)

Console> (enable)
Kerberos Realm-Server-Port entry CISCO.COM-187.0.2.1-750  deleted
Console> (enable)
```

## Mapping a Kerberos Realm to a Host Name or DNS Domain

	Task	Command
Step 1		
Step 2		

## Copying SRVTAB Files


```
set kerberos srvtab remote 187.20.32.10 /users/jdoe/krb5/ninerskeytab
```

```
set kerberos srvtab entry host/niners.cisco.com@CISCO.COM 0 932423923 1
1 8 03;;5>00>50;0=0=0
```

```
show kerberos
```

```
Srvtab Entry 2:host/niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8 00?58:127:223=::;9
Console> (enable)
```


---

	<b>set kerberos credentials forward</b>
	<b>set kerberos clients mandatory</b>

---


Console> (enable)  
Kerberos credentials forwarding disabled  
Console> (enable)  
Kerberos Local Realm not configured  
Kerberos server entries:

Kerberos Domain<->Realm entries:

Kerberos Clients NOT Mandatory  
Kerberos Credentials Forwarding Disabled  
Kerberos Pre Authentication Method set to None  
Kerberos config key:  
Kerberos SRVTAB Entries  
Console> (enable)


Console> (enable)  
Kerberos clients mandatory cleared  
Console> (enable)  
Kerberos Local Realm not configured  
Kerberos server entries:

Kerberos Domain<->Realm entries:

Kerberos Clients NOT Mandatory  
Kerberos Credentials Forwarding Disabled  
Kerberos Pre Authentication Method set to None  
Kerberos config key:  
Kerberos SRVTAB Entries  
Console> (enable)  
Kerberos server entries:

Kerberos Domain<->Realm entries:

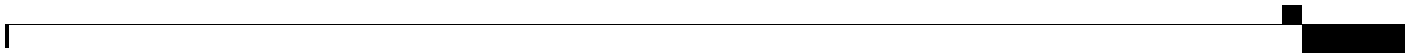
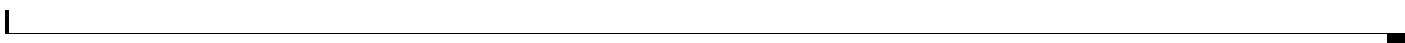
Kerberos Clients Mandatory  
Kerberos Credentials Forwarding Disabled  
Kerberos Pre Authentication Method set to Encrypted Unix Time Stamp  
Kerberos config key:  
Kerberos SRVTAB Entries  
Console> (enable)


```
kerberos> (enable)
Kerberos config key set to abcd
kerberos> (enable)
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM, Server:170.20.2.1, Port:750
Realm:CISCO.COM, Server:172.20.2.1, Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com, Realm:CISCO.COM

Kerberos Clients Mandatory
Kerberos Credentials Forwarding Disabled
Kerberos Pre Authentication Method set to Encrypted Unix Time Stamp
Kerberos config key:abcd
Kerberos SRVTAB Entries
Srvtab Entry 1:host/aspens-niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8 12151<<88?=>>3>11
kerberos> (enable)
```


```
Console> (enable)
Kerberos config key cleared
Console> (enable)
```



--	--

Console> (enable)

--	--

kerberos> (enable)  
Kerberos Local Realm:CISCO.COM  
Kerberos server entries:  
Realm:CISCO.COM, Server:187.0.2.1, Port:750  
Realm:CISCO.COM, Server:187.20.2.1, Port:750  
  
Kerberos Domain<->Realm entries:  
Domain:cisco.com, Realm:CISCO.COM  
Kerberos Clients NOT Mandatory  
Kerberos Credentials Forwarding Enabled  
Kerberos Pre Authentication Method set to None  
Kerberos config key:  
Kerberos SRVTAB Entries  
Srvtab Entry 1:host/niners.cisco.com@CISCO.COM 0 932423923 1 1 8 03;;5>00>50;0=0=0  
Srvtab Entry 2:host/niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8 00?58:127:223=::;9  
kerberos> (enable)

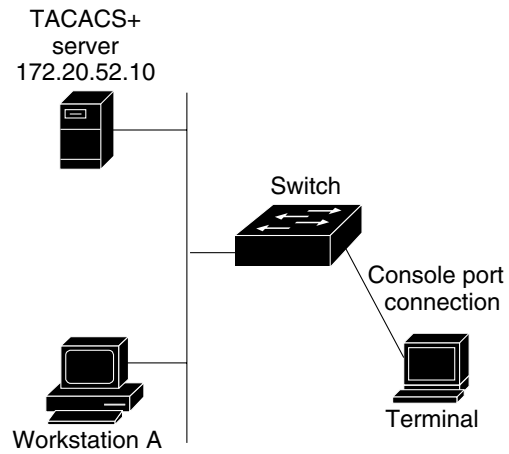
--	--

Console> (enable)  
No Kerberos credentials.  
Console> (enable)

```
Console> (enable)
Console> (enable)
```

## Authentication Example

*TACACS+ Example Network Topology*



18927

# Understanding How Authorization Works

- 
- 
- 
- 
- 

## Authorization Overview

## Authorization Events

- **Commands**—When you enable authorization for commands, the user must supply a valid username and password pair to execute certain commands. You can require authorization for all commands or for configuration (enable mode) commands only. When a user issues a command, the authorization server receives the command and user information and compares it against an access list. If the user is authorized to issue that command, the command is executed; otherwise, the command is not executed.
- **EXEC mode (normal login)**—When authorization is enabled for EXEC mode, the user must supply a valid username and password pair to gain access to EXEC mode. Authorization is required only if you have enabled the authorization feature.
- **Enable mode (privileged login)**—When authorization is enabled for enable mode, the user must supply a valid username and password pair to gain access to enable mode. Authorization is required only if you have enabled authorization for enable mode.

## TACACS+ Primary Options and Fallback Options

- **tacacs+**
- **deny**
- **if-authenticated**
- **none**

## TACACS+ Command Authorization

- **copy**
- **clear**
- **commit**
- **configure**
- **delete**
- **download**
- **format**
- **reload**
- **rollback**
- **session**
- **set**

- squeeze  
switch  
undelete


<p>console telnet</p> <p style="text-align: center;">both</p>	<p>set authorization exec enable  <span style="float: right;">console telnet both</span></p>
<p>console telnet</p> <p style="text-align: center;">both</p>	<p>set authorization enable enable  <span style="float: right;">console telnet both</span></p>
<p style="text-align: center;">console telnet</p> <p>both</p>	<p>set authorization commands enable config  <span style="float: right;">all console telnet</span>  both</p>
	<p>show authorization</p>

**tacacs+**

**deny**

**set authorization exec enable tacacs+ deny both**

Successfully enabled enable authorization.

Console>

Console> (enable) **set authorization enable enable tacacs+ deny both**

Successfully enabled enable authorization.

Console>

Console> (enable) **set authorization commands enable config tacacs+ deny both**

Successfully enabled commands authorization.

Console> (enable)

Console> (enable) **show authorization**

Telnet:

-----

	Primary	Fallback
	-----	-----
exec:	tacacs+	deny
enable:	tacacs+	deny
commands:		
config:	tacacs+	deny
all:	-	-

Console:

-----

	Primary	Fallback
	-----	-----
exec:	tacacs+	deny
enable:	tacacs+	deny
commands:		
config:	tacacs+	deny
all:	-	-

Console> (enable)


```
Console> (enable)
Successfully disabled enable authorization.
Console> (enable)
```

```
Console> (enable)
Successfully disabled enable authorization.
Console> (enable)
```

```
Console> (enable)
Successfully disabled commands authorization.
Console> (enable)
```

Console> (enable)

Telnet:

	Primary	Fallback
	-----	-----
exec:	tacacs+	deny
enable:	tacacs+	deny
commands:		
config:	tacacs+	deny
all:	-	-

Console:

	Primary	Fallback
	-----	-----
exec:	tacacs+	deny
enable:	tacacs+	deny
commands:		
config:	tacacs+	deny
all:	-	-

Console> (enable)

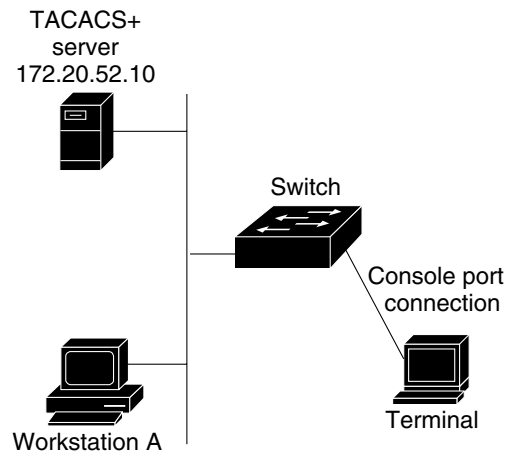
---

**set authentication login**

---

**set authentication login**

**Figure 39-4**     **TACACS+ Example Network Topology**



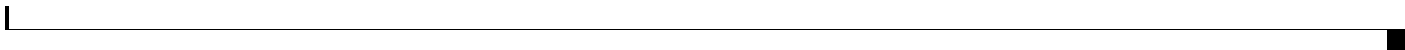
18927



---

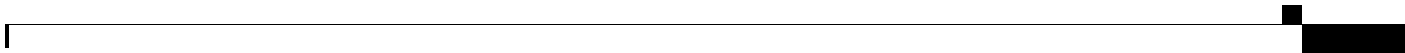
---





---

---



---

---



**Table 39-4     Accounting Default Configuration**

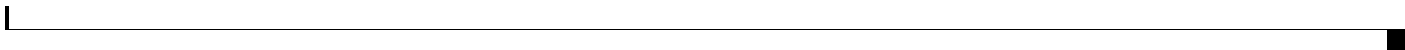


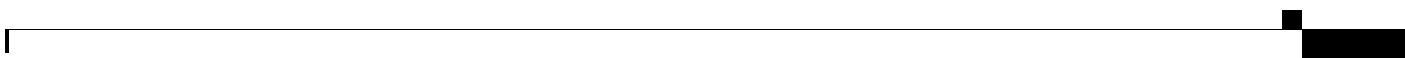

---

---



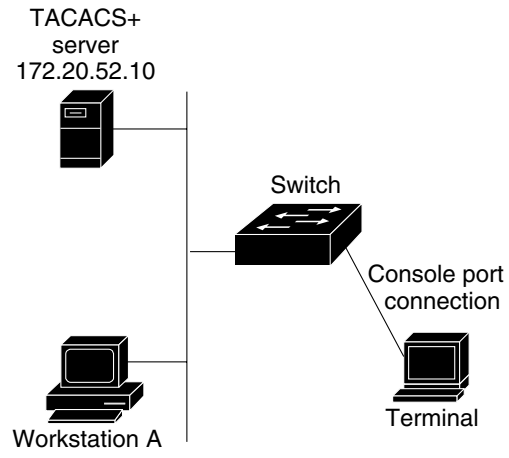




**Figure 39-5** TACACS+ Example Network Topology



18927

